Министерство науки и высшего образования Российской Федерации

Федеральное государственное автономное образовательное учреждение

высшего образования

«Уральский федеральный университет

имени первого Президента России Б.Н. Ельцина»

Институт радиоэлектроники и информационных технологий – РТФ

Школа профессионального и академического образования

Учебно-научный центр «Информационная безопасность»

**Отчет по дисциплине**

**«Операционные системы»**

**ПО ТЕМЕ: «Password Cracking»**

|  |  |
| --- | --- |
| Преподаватель | Зубков Е.В. |
| Студенты | Голованов Я.А., Коногоров Д.О., Алексеев Ю.А. |
| Специальность | Информационно-аналитические системы безопасности |
| Группа | РИ-231056 |

Екатеринбург, 2024

**Содержание**

[1. Исходные данные 3](#_Toc183729650)

[1.1 Стенд 3](#_Toc183729651)

[1.2 Процедура 3](#_Toc183729652)

[1.3 Начальные условия 4](#_Toc183729653)

[2. Процедура. 5](#_Toc183729654)

[Этап 1: Установка дополнительной утилиты John the ripper. 5](#_Toc183729655)

[Этап 2: Создание нового непривилегированного пользователя user. 6](#_Toc183729656)

[Этап 3: Объединение файлов /etc/passwd и /etc/shadow в один файл. 7](#_Toc183729657)

[Этап 4: Фильтрация словаря rockyou.txt 9](#_Toc183729658)

[Этап 5: Использование John the ripper для получения пароля пользователя user. 10](#_Toc183729659)

[Этап 6. Регистрация в системе под пользователем user. 11](#_Toc183729660)

[3. Обнаружение 13](#_Toc183729661)

[4. Смягчение последствий 13](#_Toc183729662)

# 1. Исходные данные

## 1.1 Стенд

Используемые ВМ: Виртуальная машина: Debian 12.

Дополнительно установленное ПО: John the riper – это **бесплатная программа, предназначенная для восстановления паролей по их хешам**. Основное назначение программы — аудит слабых паролей в UNIX-системах путём перебора возможных вариантов.

Установка: sudo apt-get install john

Используемые утилиты и библиотеки:

1) apt-get install - штатная утилита, предназначенная для установки дополнительных программ и пакетов.

2) adduser — штатная утилита, предназначенная, которая создает новую учетную запись пользователя.

3) cd - штатная утилита, предназначенная для изменения директории.

4) unshadow – утилита, предоставляемая программой John the ripper, которая дает возможность объединить файлы /etc/shadow и /etc/passwd.

5) cat – штатная утилита, предназначенная для демонстрации файлов на экран.

6) nano – текстовый редактор в ОС Linux.

7) John the ripper – дополнительная программа, используемая в целях подбора пароля.

## 1.2 Процедура

Тактика: Credential Access.

Техника: Password Cracking

Краткое описание техники: Для восстановления пароля используется инструмент John the ripper, который осуществляет перебор возможных вариантов пароля.

Применяется метод: Словарная атака — использование заранее подготовленного списка паролей.

Развернутое описание процедуры: Целью процедуры является восстановление пароля из хэша с использованием John the ripper. Сначала необходимо извлечь хэш пароля из системы (например, из файла /etc/shadow). Объединить файлы /etc/passwd и /etc/shadow для того, чтобы инструмент смог использовать корректные данные для взлома пароля. Затем запускается атака с использованием словаря паролей. После успешного восстановления пароля выводится его значение.

Принцип действия: John the ripper пытается сравнить хэш пароля с возможными значениями, взятыми из словаря, представляющим собой файл из набора паролей.

## 1.3 Начальные условия

Объект исследования: ОС Debian 12.

Исходные данные: Существует пользователь yarik, с помощью которого будет происходить взлом непривилегированного пользователя user.

В системе хранится хэш пароля пользователя user в файле /etc/shadow. Имеется словарь rockyou.txt с набором различных паролей. Известно, что пароль начинается на букву q и заканчивается на букву y.

Используемое программное обеспечение: John the ripper для взлома пароля пользователя.

# 2. ****Процедура.****

## ****Этап 1: Установка дополнительной утилиты John the ripper.****

**Цель этапа: Установить утилиту John the ripper**

**Описание действия: С помощью команды apt-get install устанавливаем утилиту john the ripper для дальнейшего ее использования.**

**Команда: sudo apt-get install john**

**Объяснение:**

**1) sudo – команда для единоразового использования прав “суперпользователя” Linux.**

**2) apt-get install – команда для установки пакетов, где apt – менеджер пакетов Linux.**

**3) john – необходимый пакет для взлома пароля John the ripper, john – сокращенное название данного установленного пакета John the ripper.**

****

**Результат: успешно установленная утилита John the ripper.**

## ****Этап 2: Создание нового непривилегированного пользователя user.****

Цель этапа: Создать нового пользователя, пароль которого в дальнейшем будет получен.

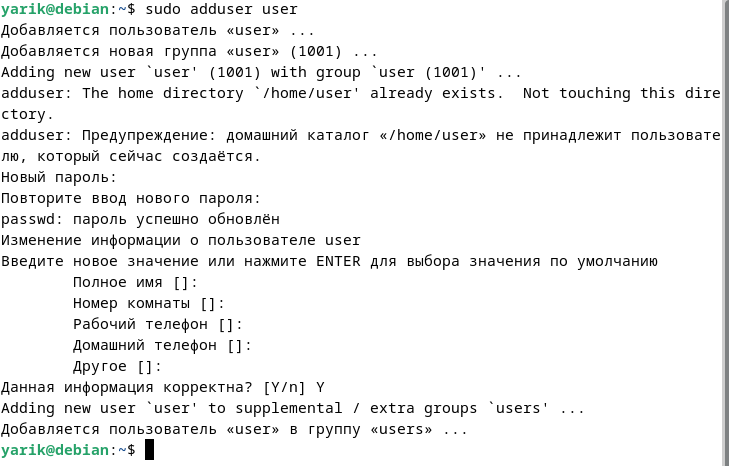
Описание действия: С помощью команды adduser создадим нового пользователя user с паролем qwerty.

Команда: sudo adduser user

Объяснение:

1) **sudo – команда для единоразового использования прав “суперпользователя” Linux.**

2) adduser – штатная утилита, которая создает пользователя user.

3) user – имя созданного пользователя.

Результат: Создался новый пользователь user с паролем qwerty.

## ****Этап 3: Объединение файлов /etc/passwd и /etc/shadow в один файл.****

**Цель этапа**: Объединить два файла для дальнейшего анализа.

**Описание действия**: Известно, что учетные записи в Linux хранятся в директории /etc/passwd, а /etc/shadow содержит информацию о паролях пользователей. Для удачного получения пароля нового пользователя user необходимо слияние 2-ух этих файлов в один. Назовем этот файл mypasswd, который сохраним в директории “Рабочий стол”.

**Команды: cd ‘Рабочий стол’, sudo unshadow /etc/passwd /etc/shadow > mypasswd, cat mypasswd.**

**Объясение:**

**1) sudo – команда для единоразового использования прав “суперпользователя” Linux.**

**2) unshadow – команда, которая предоставляется пакетом John the ripper, установленного ранее. Позволяет объединить файлы /etc/passwd и /etc/shadow в один файл.**

**3) /etc/passwd – файл, хранящий учетный записи пользователей.**

**4) /etc/shadow – файл, хранящий информацию о паролях пользователей.**

**5) > - перенаправление вывода(записи) в файл mypasswd.**

**6) mypasswd – файл, в котором содержится результат слияния.**

**7) cat – штатная утилита для демонстрации файла mypasswd.**

8) cd – штатная команда, которая меняет директорию на директорию “Рабочий стол”

****

****

****

**Результат:** Получен файл mypasswd, объединяющий файлы /etc/passwd и /etc/shadow.

## Этап 4: Фильтрация словаря rockyou.txt

Цель этапа: Отфильтровать словарь rockyou.txt для оптимизации перебора паролей.

Описание действия: С целью ускорить перебор пароля необходимо отсортировать файл rockyou.txt. Это представляется возможным благодаря тому, что известна начальная и конечная буквы пароля.

Команда: grep ‘^q….y$’ rockyou.txt > show.txt

Объяснение:

1) grep – штатная утилита, которая позволяет провести поиск по файлу с использованием шаблона.

2) > **- перенаправление вывода(записи) в файл show.txt.**

3) show.txt – файл для записи отфильтрованного словаря rockyou.txt

4) rockyou.txt – словарь с паролями.

5) ^ - в шаблоне указывает на начальный символ.

6) $ - в шаблоне указывает на последний символ символ.



Результат: получили отфильтрованный словарь.

## ****Этап 5: Использование John the ripper для получения пароля пользователя user.****

**Цель этапа**: Получить пароль пользователя user для дальнейшей регистрации в системе от его имени.

**Описание действия**: С помощью утилит встроенных в John the ripper попытаемся получить пароль пользователя user. Ранее был отфильтрован словарь rockyou.txt. Далее передадим этот файл в саму утилиту John the ripper, которая в свою очередь переберет пароли из этого файла и сравнит с расшифрованными паролями из файла /etc/shadow.

Команды: sudo john –wordlist=show.txt mypasswd –format=crypt, sudo john –show mypasswd.

Объяснение:

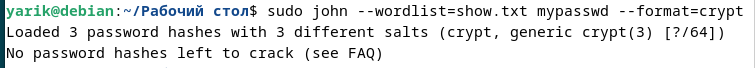
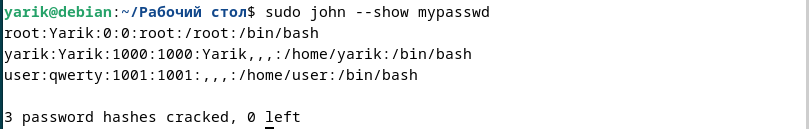
1) **sudo – команда для использования прав “суперпользователя” Linux.**

**2) john – краткое название установленного ранее пакета John the ripper, используется для обращения к этому пакету.**

**3) –wordlist – опция утилиты john, в которую передаем файл test.txt, в котором хранится пароли для перебора**

**4) mypasswd – файл, в котором ранее были объединены файлы /etc/passwd и /etc/shadow.**

**5) --format – параметр утилиты john, в который необходимо указать формат хэш-пароля. В данном случае формат - crypt.**

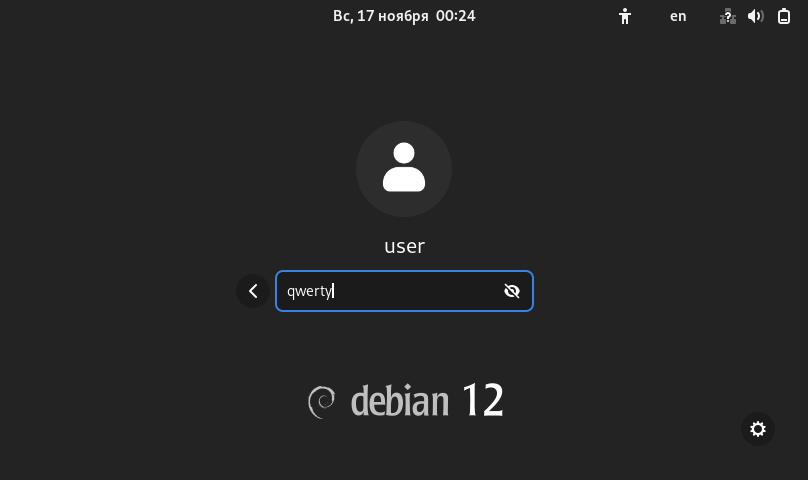
**6) –show – опция утилиты john, позволяющая вывести полученные пароли.**

Результат: получили пароль(qwerty) от пользователя user

## Этап 6. Регистрация в системе под пользователем user.

Цель этапа: Проверить, что получен верный пароль от учетной записи user.

Описание действия: Зарегистрироваться в системе под пользователем user, используя полученный пароль.



Вводим пароль, который был получен на предыдущем этапе для созданного ранее пользователя user.



Результат: удачно зарегистрировались в учетной записи user, использовав пароль qwerty.

# 3. Обнаружение

* **Описание изменений в системе**:  
  После проведения атак могут быть следующие изменения:
  + Записи в системных логах.
  + Временные файлы, созданные в процессе работы **John the Ripper**.
  + История команд в терминале.
* **Пример кода для обнаружения**: Для поиска следов работы **John the Ripper** можно использовать команды:

grep john /var/log/auth.log

Или для поиска временных файлов:

find /tmp -name "\*john\*"

# 4. Смягчение последствий

* **Рекомендации по противодействию**:
  + Использование **сложных паролей** (длинные пароли с комбинацией букв, цифр и символов).
  + Внедрение **многофакторной аутентификации** (MFA) для повышения безопасности.
  + Применение **соли** при хэшировании паролей (соль существенно усложняет атакующие методы).
  + Ограничение доступа к файлам с хэшами паролей (например, файлу /etc/shadow).